6: What is Claimed is:

1. An information-processing apparatus serving as a data-processing means for carrying out predetermined processing OP1 on input data D1 in order to produce a result of said predetermined processing as processed data D2, said information-processing apparatus comprising:

a data transform means for transforming said input data D1 by using disturbance data XI to generate transformed data H1;

a transformed-data-processing means for carrying out said predetermined processing OP1 for said input data D1 or processing different from said predetermined processing OP1 to replace said predetermined processing OP1 on said transformed data H1 in order to generate processed transformed data H2; and

a data inverse-transform means for carrying out inverse-transformation processing OP2 on said processed transformed data H2 by using processed disturbance data XO in order to generate said processed D2 which can also be obtained without transformations as a result of said predetermined processing OP1 carried out on said input data D1,

wherein said disturbance data XI and said processed disturbance data XO each have a constant or all but constant hamming weight.

2. An information-processing apparatus according to claim 1 wherein said processed disturbance data XO is generated by carrying out said predetermined processing OP1 on said disturbance data XI.

3. An information-processing apparatus according to claim 1 wherein each bit of said processed disturbance data XO and said disturbance data XI has a logic value of 0 or 1 at a probability of 50%.

4. An information-processing apparatus according to claim 1, said information-processing apparatus further having a disturbance-data and processed-disturbance-data generation means capable of generating said disturbance data XI having a constant or all but constant hamming weight and generating said processed disturbance data XO having a constant or all but constant hamming weight by execution of input-data processing defined in advance on said disturbance data XI.

5. An information-processing apparatus according to claim 1, said information-processing apparatus further having:

a disturbance-data storage means for storing a plurality of candidates for said disturbance data XI having uniform or all but uniform hamming weights; and

a disturbance-data select means for randomly selecting one of said candidates for said disturbance data XI stored in said disturbance-data storage means, wherein disturbance-data processing is carried out to process said selected candidate for said disturbance data XI in order to generate said processed disturbance data XO.

6. An information-processing apparatus according to claim 1, said information-processing apparatus further having a constant-hamming-weight-random-number generation means used for generating random numbers with uniform constant hamming weights and provided with:

a random-number generation means for generating random numbers each having a hamming weight equal to half the number of bits included in said generated random number;

a bit inversion means for inverting bits of data; and

a bit concatenation means for concatenating a random number generated by said random-number generation means with data output by said bit inversion means as a result of inversion of said random number generated by said random-number generation means.

7. An information-processing apparatus according to claim 1, said information-processing apparatus further having:

a random-number generation means for generating a random number to be used as said disturbance data XI;

a hamming-weight computation means for computing a hamming weight of a random number generated by said random-number generation means;

a hamming-weight examination means for examining said hamming weight computed by said hamming-weight computation means; and

a constant-hamming-weight assurance means for requesting said random-number generation means to generate another random number for said hamming-weight examination means' result of examination indicating an inspected hamming weight not equal to a target hamming weight.

8. An information-processing apparatus according to claim 1, said information-processing apparatus further having a constant-hamming-weight-random-number generation means used for generating random numbers with uniform constant hamming weights and provided with:

a constant-hamming-weight and constant-fractional-bit-count random-number generation means used for generating partial random numbers with uniform constant hamming weights and uniform bit counts each equal to a fraction of the bit count of a final random number to be generated;

a random-number-generation control means for controlling said constant-hamming-weight and constant-fractional-bit-count random-number generation means to generate partial random numbers till a sum of bit counts of said partial numbers equal to said bit count of said final random number; and

a data concatenation means for concatenating said partial random numbers generated by said constant-hamming-weight and constant-fractional-bit-count random-number generation means to result in said final random number.

9. An information-processing apparatus comprising:

a storage unit having a program storage sub-unit for storing a program and a data storage sub-unit for storing data;

a central processing unit for carrying out predetermined processing by execution of said program;

an input-data-processing means for looking up a table for an entry pointed to by input data D1 used as an index of said table and outputting said entry as processed data;

a transformed table generated by transformation of indexes of said table by using first disturbance data X1i with an all-time constant or all-time all but constant hamming weight and transformation of said table's entries pointed to by said indexes by using second disturbance data X2i with an all-time constant or all-time all but constant hamming weight;

a data transform means for transforming said input data D1 by using said disturbance data X1i to generate transformed data H1;

a transformed-table access means for looking up said transformed table for processed transformed data H2 pointed to by said transformed data H1 used as an index of said transformed table; and

a data inverse-transform means for carrying out inverse transformation on said processed transformed data H2 by using said second disturbance data X2i in order to generate said processed D2 which can also be obtained without transformations as a result of input-data processing carried out on said input data D1.

10. An information-processing apparatus according to claim 9, said information-processing apparatus further having a table transform means for creating said transformed table by using:

a first constant-hamming-weight-random-number generation means for generating said first disturbance data X1i;

a second constant-hamming-weight-random-number generation means for generating said second disturbance data X2i;

said first disturbance data X1i;

said second disturbance data X2i; and

said table,

wherein indexes of said table are transformed by using said first disturbance data X1i and contents of said table are transformed by using said second disturbance data X2i to generate said transformed table.

11. An information-processing apparatus according to claim 9, said information-processing apparatus further having:

a first-disturbance-data storage means for storing in advance a plurality of numbers having uniform and constant or all but uniform and all but constant hamming weights;

a first-disturbance-data select means for randomly selecting one of said numbers stored in said first-disturbance-data storage means to be used as said first disturbance data X1i;

a second-disturbance-data storage means for storing in advance a plurality of numbers having uniform and constant or all but uniform and all but constant hamming weights;

a second-disturbance-data select means for randomly selecting one of said numbers stored in said second-disturbance-data storage means to be used as said second disturbance data X2i; and

a table transform means for creating said transformed table by transformation of indexes of said table by using said first disturbance data X1i and transformation of contents of said table by using said second disturbance data X2i.

12. An information-processing apparatus according to claim 9 wherein:

first disturbance data with a constant hamming weight is prepared in advance as a candidate for said first disturbance data X1i;

second disturbance data with a constant hamming weight is prepared in advance as a candidate for said second disturbance data X2i;

a pair consisting of said first disturbance data and said second disturbance data is used in transformation to create said transformed table;

a plurality of such pairs is created;

the same plurality of such transformed tables is created by using said pairs and stored in a transformed-table storage means along with said pairs by associating said transformed tables with said pairs; and

a means is provided for selecting a set consisting of first disturbance data, second disturbance data and a transformed table from said transformed-table storage means to be used as said first disturbance data X1i, said first disturbance data X2i and said transformed table.

13. An information-processing apparatus serving as a data-processing means for carrying out a lookup operation on a table, carrying out data processing on a lookup-operation result and outputting a result of said data processing as processed data, said information-processing apparatus comprising:

a data transform means for transforming input data

D1 by using first disturbance data X1I to generate transformed data H1,

a transformed-table access means for looking up a transformed table for transformed data H2 pointed to by said transformed data H1 used as an index of said transformed table;

a transformed-data-processing means for processing said transformed data H2 to produce processed transformed data H3; and

a data inverse-transform means for carrying out inverse transformation on said processed transformed data H3 by using processed second disturbance data X2o in order to generate processed D2 which can also be obtained without transformations as a result of said lookup operation carried out on said table by using said input data D1 and said data processing carried out on said result of said lookup operation,

wherein:

said first disturbance data X1i has an all-time constant or all-time all but constant hamming weight;

second disturbance data X2i has an all-time constant or all-time all but constant hamming weight and provides a constant or all but constant hamming weight to a result of data processing carried out on said second disturbance data X2i after said lookup operation, that is, processed second disturbance data X2o obtained as a result of said data processing carried out on said second disturbance data X2i also has an all-time constant or all-time all but constant hamming weight as well; and

indexes of said table are transformed by using said first disturbance data X1i whereas said table's contents pointed to by said indexes are transformed by using said second disturbance data X2i to create said transformed table.

14. An information-processing apparatus according to claim 13, said information-processing apparatus further having:

a first constant-hamming-weight-random-number generation means for generating said first disturbance data X1i;

a second constant-hamming-weight-random-number generation means for generating said second disturbance data X2i;

a disturbance-data-processing means for processing said second disturbance data X2i to produce said transformed second disturbance data X2o;

a hamming-weight examination means for computing a hamming weight of said processed second disturbance data X2o and requesting said second constant-hamming-weight-random-number generation means to generate another value of said second disturbance data X2i in the case of an improper hamming weight of said processed second disturbance data

X2o; and

a table transform means for creating said transformed table by transformation of indexes of said table by using said first disturbance data X1i and transformation of contents of said table by using said second disturbance data X2i.

15. An information-processing apparatus according to claim 13, said information-processing apparatus further having:

a first-disturbance-data storage means for storing a plurality of numbers having uniform and constant or all but uniform and all but constant hamming weights;

a first-disturbance-data select means for randomly selecting one of said numbers stored in said first-disturbance-data storage means to be used as said first disturbance data X1i;

a second-disturbance-data storage means for storing a plurality of numbers having uniform and constant or all but uniform and all but constant hamming weights as well as providing uniform and constant or all but uniform and all but constant hamming weights to results of disturbance-data processing carried out on said numbers;

a second-disturbance-data select means for randomly selecting one of said numbers stored in said second-disturbance-data storage means to be used as said second disturbance data X2i;

a second-disturbance-data processing means for carrying out said disturbance-data processing on said second disturbance data X2i to generate said processed second disturbance data X2o; and

a table transform means for creating said transformed table by transformation of indexes of said table by using said first disturbance data X1i and transformation of contents of said table by using said second disturbance data X2i.

16. An information-processing apparatus according to claim 13, said information-processing apparatus further having:

a first-disturbance-data storage means for storing a plurality of numbers having uniform and constant or all but uniform and all but constant hamming weights;

a first-disturbance-data select means for randomly selecting one of said numbers stored in said first-disturbance-data storage means to be used as said first disturbance data X1i;

a second-disturbance-data and processed-second-disturbance-data storage means for storing a plurality of pairs each consisting of second disturbance data and processed second disturbance data, wherein said second disturbance data has a constant or all but constant hamming weight and provides a constant or all but constant hamming weight to said processed second disturbance data obtained as a result of disturbance-data processing carried out on said second disturbance data;

a second-disturbance-data and processed-second-disturbance-data select means for randomly selecting one of said pairs each consisting of second disturbance data and processed second disturbance data from said second-disturbance-data and processed-second-disturbance-data storage means to be used as a pair of said processed second disturbance data X2o and second disturbance data X2i; and

a table transform means for creating said transformed table by transformation of indexes of said table by using said first disturbance data X1i and transformation of contents of said table by using said second disturbance data X2i.

17. An information-processing apparatus according to claim 13, said information-processing apparatus further having:

a second-disturbance-data, processed-second-disturbance-data and transformed-table storage means for storing a plurality of sets each consisting of a candidate for said first disturbance data X1i, a candidate for said processed second disturbance data X2o and a candidate for said transformed table; and

a second-disturbance-data, processed-second-disturbance-data and transformed-table select means for randomly selecting one of said sets each consisting of a candidate for said first disturbance data X1i, a candidate for said processed second disturbance data X2o and a candidate for said transformed table from said second-disturbance-data, processed-second-disturbance-data and transformed-table storage means to be used as a set of said first disturbance data X1i, said processed second disturbance data X2o and said transformed table,

wherein:

said candidate for said transformed table is created by transformation of indexes of said table by using said candidate for said first disturbance data X1i and transformation of contents of said table by using said candidate for said second disturbance data X2i;

said candidate for said processed second disturbance data X2o is obtained as a result of processing carried out by disturbance-data processing means on said candidate for said second disturbance data X2i;

said candidate for said first disturbance data X1i has a constant hamming weight;

said candidate for said second disturbance data X2i has a constant hamming weight as well; and

said candidate for said processed second disturbance data X2o also has a constant hamming weight even after said processing carried out by said disturbance-data processing means.